PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G07B 17/00 — A1

(11) International Publication Number: WO 00/55817

(43) International Publication Date: 21 September 2000 (21.09.00)

(21) International Application Number: PCT/GB00/01041

(22) International Filing Date: 20 March 2000 (20.03.00)

(30) Priority Data:
9906293.7 18 March 1999 (18.03.99) GB

(71) Applicant *(for all designated States except US)*: THE POST OFFICE [GB/GB]; Royal Mail House, 148 Old Street, London EC1V 9HQ (GB).

(72) Inventors; and

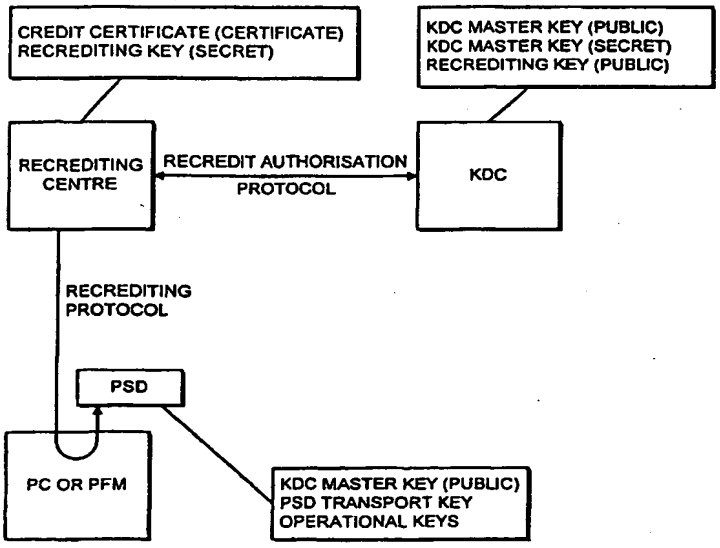
(75) Inventors/Applicants *(for US only)*: COWARD, David [GB/GB]; Royal Mail Technology Centre, Wheatstone Road, Dorcan, Swindon SN3 4RD (GB). COOK, Richard [GB/GB]; Royal Mail Technology Centre, Wheatstone Road, Dorcan, Swindon SN3 4RD (GB). BOSWELL, Tony [GB/GB]; The Post Office, Legal Services, Impact House, 2 Edridge Road, Croydon CR9 1PJ (GB). PERKINS, Richard [GB/GB]; The Post Office, Legal Services, Impact House, 2 Edridge Road, Croydon CR9 1PJ (GB).

(74) Agents: KINSLER, Maureen et al.; Kilburn & Strode, 20 Red Lion Street, London WC1R 4PJ (GB).

(81) Designated States: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
With amended claims.

(54) Title: IMPROVEMENTS RELATING TO POSTAL SERVICES



(57) Abstract

A method for permitting a postal authority to maintain control over transactions in a franking system, the postal franking system comprising postal franking means (PFM) including a postal security device (PSD) which maintains in a secure manner funds credit data; a credit authorisation facility (CAF) and a recrediting facility (RF) for issuing a funds credit to the PSD, wherein the method comprises: (a) the CAF issuing to the RF in a limit of funds which may be credited to the PFD; (b) the PFM making to the RF a request for personal credit; and (c) the RF checking on the funds available to the PSD and providing to the PSD, if available, further credit by means of a message encrypted and/or authenticated form.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

IMPROVEMENTS RELATING TO POSTAL SERVICES

The present invention relates to postal services, and franking systems therefor.

Franking systems in which the frank indicating the postage revenue paid on a mail piece is applied by the user, are in common use. One system comprises a machine which franks letters to desired rates and which records the total postal value franked in a counting mechanism. It has been proposed to put the counting mechanism in a detachable unit which periodically would be taken to a local postal station and the total value of the post indicated in the unit be recorded, and payment made. The postal station subsequently makes payment to the postal authority. Clearly such a system is inefficient in terms of operator time, requiring the operator to visit the local postal station

Another type of proposed franking system is where the supplier of the franking machine handles the recrediting transactions remotely. Thus recredit payments are made at periodic intervals direct to the supplier of the equipment by payment through the post or by electronic funds transfer. Whilst this avoids the necessity of visiting a local postal station, it is the responsibility of the supplier to settle with the postal authority the total value of the letters posted which have been franked by means of the supplier's equipment. This is disadvantageous from the point of view of the postal authority, since they have to rely entirely on the equipment supplier for correct reimbursement.

It is an object of the present invention to overcome or at least reduce the above problems.

The present invention is based on communication between the user and a recrediting facility (RF) responsible for transferring postal credit to the user to permit the user to use the postal service up to the limit of the credit. The postal service itself, can receive the franked mail from the user and maintain control over supply of postal credit from the RF to the user.

In such a communication system. security and reliability of postal credit information is essential. Thus it is important that the transfer of funds and the dedication of funds to mail pieces, is secure and is immune to fraudulent manipulation. so far as possible. However the franking system must be as flexible as possible for widespread adoption. Thus the means of communication between the user and various elements of the system must be open. However, an open-access environment is inherently insecure and is naturally in conflict with the need for security. It is therefore essential to place the emphasis for security on the transmitted data.

The user has a special purpose postal security device (PSD) for use with, or forming part of, a postal franking means (PFM) which may be a special purpose machine) or a suitably adapted personal computer (PC). The PSD keeps an account of funds available for the franking of mail pieces by the PFM controlling a suitable printer. The PSD communicates with the rest of the system through the PFM. The PSD is credited with funds from the RF. Mail pieces that have been franked by the printer are received at the mail centre (MC) where they are scanned, decoded and funds associated with the mail piece are reconciled. The frank preferably includes a bar code (although it may be a sequence of alphanumerics) carrying information as to the value of the frank,

the identity of the user and other cryptographically protected information to permit a mail centre (MC) to identify unambiguously the user and to verify the validity of the frank. In this way the MC may also monitor the activities of the user.

The postal security device (PSD) communicates with the RF. It may take the form of a secure device, e.g. a smartcard, PC card or a dongle, with an interface to the PC or PFM. The PSD holds postal credit, and the RF serves to recredit on request by recrediting the PSD to a requested value in accordance with the certified credit available from the RF for that PSD. Recrediting and payment preferably take place via a communication link, but can also be by physically visiting the recrediting RF or a post office linked to the RF with the PSD. In any event, the transaction or transactions between the RF and the PSD take place in a secure manner with appropriate identification, verification and encryption of data transferred between the RF and PSD.

The RF can also control the transfer of funds to the PSD, providing security keys for encrypted communication and/or remote PSD function modification or disablement in the event of evidence of attempted tampering and transfer other information such as tariff charges and promotional messages. The RF may be separately managed from the provider of the franking and/or PSD equipment for part of the turn key service. However, overall control of fund allocation is maintained by the postal services supplier.

A credit authorisation facility (CAF), usually part of the postal authority, or at least under control of the postal authority, is provided for authorising the RF to credit each particular user PSD to a certain credit limit. The RF may request the

CAF to authorise the further credit of funds to any particular user PSD. Communication exchanges between the CAF and the RF may be available to open access or by way of secure data links. The credit authorisation is normally given to the RF in the form of a credit certificate (CC).

In accordance with one embodiment of the invention, a credit certificate may include information as to a credit limit, a recrediting public key for the RF, and a digital signature which comprises a hash of the information in the CC, encrypted by a private key in the credit authorisation facility. The digital signature is appended to the data. (Alternatively where symmetric keys are employed for encryption, a message authentication code is added). The RF stores the credit information and forwards the credit information to a user PSD in accordance with a funds request protocol. Since the RF does not possess the CAF secret key, it cannot generate a digital signature (or MAC) and possibly manipulate the allocated funds. Thus, the CC is forwarded as part of a funds request response essentially unmodified.

In the funds request protocol, a user PSD provides the PFM with its PSD Id, an indicator of the keys it currently holds including the public key version of the CAF key pair, the total value credited and the total value spent. The PC adds to this a request for a specific amount of credit and transmits it all to its associated RF. This request is normally in unencrypted form and unsigned. The RF responds with a message including information taken from the CC held in relation to the PSD. The public key of the CAF stored in the PSD is employed in order accurately to verify the signature in the credit certificate transmitted from the RF to the PSD. This provides a highly reliable means of credit authorisation. The recrediting key is used to verify the signature of the

remaining message.

The CAF preferably includes a key distribution centre (KDC) (alternatively this may be a separate part of the postal service). The strength of the KDC determines the integrity of the security of the system. It co-ordinates a supply of keys to the RF, PSD, and MC. Security of data is crucial to the integrity of the system because of the openness of the means of communication between the system components. Because the communication paths may be insecure, the data transmitted along these paths has to be secured by the use of sufficiently strong encryption techniques. The encrypted keys may be public and private as preferred with current technology, triple-DES encrypted keys with cipher block chaining with an initialisation vector.

Accordingly, in a first aspect, the invention provides a postal franking system comprising:

a postal franking system comprising:

post franking means including a postal security device (PSD) which maintains in a secure manner funds credit data;

a recrediting facility (RF) arranged to receive funds credit authorisation and to issue a funds credit response to the PSD in an encrypted and/or signed or authenticated form;

a credit authorisation facility (CAF) for issuing said funds credit authorisation for the PSD to be held by the RF; and

the post franking means being operable to issue a funds credit request to the RF, and to receive the credit response.

In a second aspect, the invention provides a method of postal funds credit to

users in a postal franking system, the postal franking system comprising:

a method of issuing postal credit values to users in a postal franking system, the postal franking system comprising:

post franking means (PFM) including a postal security device (PSD) which maintains in a secure manner funds credit data;

a credit authorisation facility (CAF);

a recrediting facility (RF) for issuing a funds credit to the PSD:

the method comprising the following steps:

(a) the CAF issuing to the RF a limit on funds which may be credited to the PSD;

(b) the PFM making to the RF a request for postal credit: and

(c) the RF checking on the funds available to the PSD and providing to the PSD, if available, further credit by means of a message encrypted and/or authenticated form.

As mentioned above, the user may make to the RF a request for postal credit by transmitting from the associated PFM, for example a PC, a request in unencrypted form. The recrediting facility replies with a credit allocation message which is signed by the RF. The message preferably includes a credit certificate, which is signed, using a secret key of the credit authorisation facility (CAF).

In a third aspect of the present invention there is provided a method of issuing postal credit values to users in a postal franking system, the postal franking system including:

postal franking means (PFM) including a postal security device (PSD) for maintaining in a secure manner funds credit data;

a recrediting facility(RF) for issuing a funds credit to the PSD;

wherein the method comprises:-

(a) the PFM issuing to the RF an unsigned request message for the reallocation of funds to the user PSD;

(b) in response thereto the RF providing a response message including a new reallocation of funds and the message including a signature based on encrypting a hash of the information in the message with a key of the RF and including credit information having a second signature formed by encrypting a hash of the credit information using a second key;

(c) the PSD means verifying the response message and verifying the message using the first key of the RF and the second key; and

wherein the user PSD stores in a secure manner the revised funds allocation information.

In a further aspect, the invention provides a method of updating keys for use in a secure postal franking system, as follows:

(i) in a first time period a first set of key versions is allocated, and a key version is selected from the first set; each key version identifying a collection of keys;

(ii) deriving keys held by a security device from these keys which are determined from the identifying key version and from a security device identifier, and during this first time period if the security device is operated, the updated key is transferred thereto;

(ii) during a second time period, overlapping in part with the first time period, a second set of key versions is provided, and an updated key version is selected from the second set; and

wherein during the second time period the security device key is changed either upon operation or following a key change request.

Brief Description of the Drawings

A preferred embodiment to the invention will now be described merely by way of example with reference to the accompanying drawings wherein:-

Figure 1 is a schematic block view of the postal franking system incorporating the present invention;

Figure 2 is a schematic block diagram showing the elements of the system of Figure 1 which are specific to the preferred embodiment of the invention;

Figure 3 is a conceptual block diagram indicating a recrediting protocol in accordance with the invention for recrediting a PSD from a RF;

Figure 4 is a flow diagram illustrating the processing of a recredit response message in the protocol of Figure 3;

Figure 5 is a flow diagram illustrating the processing of a key update block in the recredit response of Figure 4;

Figure 6 is a flow diagram illustrating the processing of the PSD control block in the recredit response of Figure 4;

Figure 7 is a flow diagram illustrating the processing of the recredit response block in the recredit response of Figure 4;

Figure 8 is a flow diagram illustrating the processing of the credit certificate in the recredit response of Figure 4;

Figure 9 is a block diagram illustrating the protocol for authorising a recredit centre or station from the credit authorisation centre or key distribution centre to recredit a specific PSD;

Figure 10 is a conceptual data flow diagram illustrating essential elements of data flow in the recredit authorisation protocol and recrediting protocol of Figures 3 and 9: and

Figure 11 is a schematic diagram of a means for generating updated keys from a Key Distribution Centre.

Description of the Preferred Embodiments

Referring to Figure 1 which is a block diagram of the overall postal system, each customer or user 2 possesses a postal franking means (PFM) comprising a PC 4 and a printer, or a dedicated postal franking machine for producing franking indicia on letters. Typically, the indicia are in the form of machine readable and/or human readable data on an envelope or mailing label.

Before generating mail, the user must first have postal credit available. This is stored and maintained in a postal security device (PSD) 8 which forms part of the PFM and is in communication with the PC. To recredit a PSD, credit is transferred on-line, e.g. via a modem link, to the PC from a recrediting facility (RF) 6.

The user uses the credit value maintained in the PSD to print proof of payment indicia on to envelopes or labels. These indicia contain a machine readable code at least partly in encrypted form and human readable data. When the mail reaches a mail centre (MC) 10 the indicia are scanned and payment is validated.

When cryptographic keys are unique to a PSD, a successful attack on a single PSD does not affect the cryptographic keys of the other PSDs. A well designed PSD should delete the cryptographic keys in response to an attack, which would render it unusable.

A PSD would be expected to have a secure real time clock so that timing constraints could be utilised when required.

The generation of encrypted dynamic information, and the subsequent printing of that information onto the envelope, is not, in itself, a secure system. At some stage the information needs to be decrypted and reconciled with expected or known customer and item information. The reconciliation process requires that the infrastructure for scanning is in place and that the information flows required for decryption and customer account checking are enabled. The encryption keys would be generated and distributed by the postal service, so the communication infrastructure to support the key management system described above would also need to be enabled.

Each mail customer possesses one or more PSDs which can be used to produce indicia in conjunction with either a PC and a printer or with a dedicated postal franking machine (PFM). As discussed above, the PSD is the only piece of customer equipment that is relied upon for providing security.

Each customer obtains postal value, which is used for generating indicia, from RF 6. This is transferred on-line onto the PSD. A RF may be run by organisations other than the originator of postal value. The system permits them to be given a limited amount of trust.

A RF is given authorisation for distributing credit to customers from a credit authorisation facility (CAF) : hereinbelow alternatively referred to as a Key Distribution Centre (KDC). CAFs or KDCs are operated in highly secure conditions by a trusted organisation.

The security of cryptographic keys at the MC 10 can be monitored by checking samples of indicia at checking stations 12 by automated equipment.

For generation of indicia, the PSD 8 contains a main franking key and a check franking key. The particular set of keys is identified by a PSD identification code and a key versions identifier.

The MC contains franking master keys and transport master keys which are held in a key distribution centre (KDC) 14 for distribution. In this embodiment the KDC also serves as a credit authorisation facility (CAF) although it could be separately managed.

The check franking master keys are used as a back up check on indicia to detect compromise of the main franking master keys. Each of the components shown contains cryptographic keys and uses them to perform cryptographic operations. Keys must be held by the PSD in a physically sealed environment to which

nobody has physical access and to which electronic access is limited.

A RF is given authorisation for distributing credit to customers from the KDC 14. The KDC 14 operates in a highly secure condition under the control of a trusted organisation, and, for the purposes of the present invention, forms part of the postal authority, even though the organisation may be a separate legal entity from the postal authority.

The cryptographic keys held by the various elements are indicated in Figure 1. Each key is symmetric or has a public key part and a secret key part, and implements a DES algorithm. In more detail, the keys and data are as follows:-

PSD Keys and Data

Data item	**Description**
Check Franking Key	128-bit Triple-DES key Unique to each PSD
KDC Master Key (public)	1024-bit (or larger) RSA key
Main Franking Key	128-bit Triple-DES key Unique to each PSD
PSD Transport Key	128-bit Triple-DES key Each PSD has a unique PSD Transport Key
KDC Master Key Version	8-bit data field
Key Versions	10-bit field indicating the versions of the

	Main Franking Master Key, the check Franking Master Key, the Confidentiality Key and PSD Transport Master Key
Total Value Credited	The total value that has ever been credited to a PSD. A recredit operation adds to the total value credited. The value never decreases.
Total value Spent	The total value that has ever been spent by a PSD. Creation of an indicium adds to the total value spent.

Recrediting Keys and Data

Data item	Description
Credit Certificate	
Recrediting Key (secret)	1024-bit (or larger) RSA key Unique to the RF. Each RF can have any number of Recrediting Keys.

MC Automation Keys and Data

Data item	Description
KDC Master Key (public)	1024-bit (or larger) RSA key
KDC Master Key Version	8-bit data field
Key Versions	10-bit data field indicating the versions of the Main Franking Master Key and the Confidentiality Key.

KDC Keys and Data

Data item	Description
KDC Master Key	1024-bit (or larger) RSA key Shared
Main Master Key Version	8-bit data field
Main Franking Master Key	192-bit Triple-DES symmetric key
Key Versions	10-bit data field indicating the versions of the Main Franking Master Key, the Check Franking Master Key, the Confidentiality Key, PSD Transport Master Key.

Referring to Figure 2, the elements of Figure 1 which are specific to the preferred embodiment of the present invention are shown. The components, data held in them and the protocols between them as shown in Figure 2 may be summarised as follows:

PSD

Each PSD contains:

- a PSD Identifier, a unique identifier for the PSD
- a number of operational keys, which are used for purposes such as producing indicia and a key for decrypting encrypted keys
- Key Versions, which are identifiers for the versions of these keys and form an increasing sequence (modulo k, where k is a constant in the system)

- The public part of the KDC Master Key, which is used to verify signatures of Credit Certificates. and then data on which the key must be changed.

The PSD also contains two registers:

- the Total Value Credited, the total value that has ever been credited to the PSD
- the Total value Spent, the total value of indicia that have ever been produced by the PSD.

The value available to the PSD is the difference between the Total Value Credited and the Total Value Spent. Creation of an indicium adds to the total value spent. A recredit operation adds to the total value credited. Neither of these values ever decreases.

A PSD's keys are updated on-line on a regular basis and/or on suspected key compromise.

The PSD does all the encryption for the user. The KDC has a master key and the PSD has a public version of the master key. The PSD has "a key version identifier" to identify which version of the master key it possesses. When changing a key held by a PSD the key version identifier for the new key is also loaded in the PSD.

RF Centre Keys and Data

The RF 6 contains:

- a set of Credit Certificates (see below), at least one for each PSD for which they are authorised to recredit to a limit specified in the certificate.
- one or more secret Recrediting Keys which are unique to the recrediting Centre and are used to sign recrediting data sent to PSDs.
- the Maximum Total Value Credited for each PSD that may use the RF. which includes the amount that the RF is authorised to provide to the PSD.
- appropriate accounting data.

A Credit Certificate includes:

- a Credit Certificate Indicator
- the PSD Id for the respective PSD accredited through that RF.
- Key Versions which are indicator of the current set of keys that should be held by the PSD
- a Limit of Total value credited that the RF can assign to the PSD using this Credit Certificate.
- a Recrediting Public Key, the public key corresponding to the private key used by the RF to sign the recrediting data.
- a signature covering the data in the Credit Certificate using the KDC master Secret key.

KDC Keys and Data 14

The KDC 14 contains:

- KDC Master keys which it uses to sign Credit Certificates
- Transport keys used for securing confidential data for each PSD
- Key Versions.

Recrediting Protocol

The recrediting protocol adds new value to a PSD, and transmits control messages and changes to PSD keys. The protocol is illustrated in Figure 3. It is initiated by the user 2 of the PC or PFM and communicates with the RF.

Message Sequence

The aspects of the recrediting protocol that are relevant to cryptography are contained in a Recredit Request Message from the PFM to the RF and a Recredit Response Message from the RF to the PFM. The PFM requests some basic information about the PSD's state which it combines with the value requested and sends to the Recrediting Centre. The response from the Recrediting Centre is passed unmodified through the PSD. Recrediting minimises the value held on a PSD. The only way that value can be taken from a PSD is by producing indicia.

In addition to a recrediting instruction for the PSD the Recredit Response Message can contain PSD control instructions and key update messages. The

control commands can be used to disable a PSD. The key updates must be entered into the PSD before the recrediting instruction.

Key updates should take place from time to time and new keys are distributed to PSDs during recrediting operations. This ensures that any PSD that needs recrediting will have the latest keys (helping to control key lifetimes) and can also allow timely key update in the case of suspected key compromise.

The recrediting protocol has the following properties:

- Unauthorised recredits are prevented since the PSD checks the Total Value Credited in an incoming message against the Limit of Total Value Credit in the Credit Certificate.
- Recrediting value cannot be lost because a request can be reissued.
- Recrediting cannot take place if a PSD holds keys that need to be replaced.
- Recredits must have originated from an authorised RF because of the public key in the credit certificate.
- Multiple recredits are prevented because use of the same message more than once in a PSD has no effect.

Note that the protocol relies upon knowledge of the Maximum Total value Credited at a RF. The Maximum Total Value Credited is incremented as a result of a payment associated with the PSD resulting in an extension of credit. If PSDs possess an initial credited value, this must be known by the RF.

PSD Information Message

On request from a PC or PFM, a PSD returns the following data:

- the PSD Id of the PSD
- Key Versions held by the PSD
- KDC Master Key Version held by the PSD
- Total Value Credited held by the PSD
- Total Value Spent held by the PSD

This message is used by the PFM to construct a Recredit Request Message.

Recredit Request Message

The PFM appends information to the PSD Information Message about the value to be credited, to give:

- PSD Id, from the PSD information Message
- Key Versions, from the PSD Information Message
- KDC Master Key Version, from the PSD Information Message
- Total Value Credited, from the PSD Information Message
- Total Value Spent, from the PSD Information Message
- Requested Value, a positive financial value to be added to the PSD's Total Value Credited.

The RF accepts a Recredit Request Message if there is sufficient credit associated with the PSD Id, i.e. if Requested Value + Total Value Spent ≤ min

(Maximum Total Value Credited, Limit of Total Value Credited). Note that a Recredit Response Message can be sent out any number of times, even for the same Total Value Credited and different Requested Values.

Recredit Response Message

In response to a valid Recredit Request Message a RF returns a Recredit Response Message to the PFM. A Recredit Request Message consists of one or more blocks:

- Key Update Block. (a possibly empty sequence)
- PSD Control Block. (optional)
- Recredit Response Block.

The PFM receiving this message must process each part of the message where present in the order in which it appears in the message. The order of processing is illustrated in Figure 4.

Key Update Block

The Key Update Block contains a new value for keys held by the PSD:

- Key Update Indicator, a unique identifier
- the PSD Id of the intended destination PSD
- new Key Versions, for the updated keys
- the Encrypted Keys, to be the replacements
- a signature using the KDC master key covering the above data. A key

update block may contain a new KDC master key. The version of the KDC master key used to sign a key update block should be the one expected before the update.

On receiving a Key Update Block the PSD:

- checks the Key Update Indicator
- checks that the PSD Id is correct
- checks that the new Key Versions do not cause old keys to be reinstalled. i.e. that

(new Key Versions – Key Versions) mod $k < x$,

where x is a value configured into the PSD and $x \ll$ key

- verifies that the signature on the message is correct.
- Updates all of its keys with those in the Key Block and replaced the key Versions indicator with the new Key Versions indicator.

This is illustrated in Figure 5.

PSD Control Block

A PSD Control Block is a facility intended for controlling PSDs remotely, for example disabling the PSD. The PSD Control Block contains

- PSD Control Block Indicator, a unique identifier
- the PSD Id of the intended destination PSD
- an Instruction, a value indicating the action that the PSD should perform, e.g. to cease issuing indicia

- a signature using the KDC master key covering the above data.

On receiving a PSD Control Block the PSD:

- checks the PSD Control Block Indicator
- checks that the PSD Id is correct
- checks that the Instruction is recognised
- verifies that the signature on the message is correct
- performs the instruction.

This is illustrated in Figure 6.

Recredit Response Block

A Recredit Response Block comprises

- Recredit Response Indicator, a unique identifier
- the PSD Id of the intended destination PSD
- the Key versions after all key update operations have been performed
- New Total Value Credited, equal to the sum of the supplied Total Value Credited and the Requested Value
- a signature using the Recrediting Key covering the above data
- a Credit Certificate for the Recrediting Key used in the above signature.

The PSD only accepts the Recredit Response Block if:

- the block has a Recredit Response Indicator
- the PSD Id field in the Recredit Response Block matches that held in the

PSD

- the Key versions field from Recredit Response Block matches that held in the PSD
- the Total Value Credited is greater than the equivalent field held in the PSD
- the Limit of the Total Value Credited is greater than the equivalent field held in the PSD
- the Limit of the Total Value Credited in the Credit Certificates is not less than the New Total Value Credited in the Recredit Response Block
- the Recrediting Public Key can verify the signature in the Recredit Response Block
- the KDC Master Public key held by the PSD can verify the signature in the Credit Certificate. If a KDC key update is contained in the message, the new key should be used to check the signature.

If so, the PSD adds the Credit requested to its Total Value Credited.

This is illustrated in Figures 7 and 8.

Recredit Authorisation Protocol

The recredit authorisation protocol enables RFs to obtain Credit Certificates for new PSDs, periodically to obtain increased limits on their Credit Certificates or to update their Credit Certificates for use with a new KDC Master Key. The protocol is illustrated in Figure 9.

Message Sequence

The recredit authorisation protocol consists of two messages.

Before this protocol can be used the KDC needs to possess an authentic copy of the Recrediting Public Key. This is by means outside the scope of this protocol.

Recredit Authorisation Request Message

A RF sends in a secret form a Recredit Authorisation Request Message to the KDC to request a new Credit Certificate.

Recredit Authorisation Request Message

A RF sends a Recredit Authorisation Request Message to the KDC to request a new Credit Certificate. A Recredit Authorisation Request Message contains:

- Recredit Authorisation Request Indicator, a unique identifier
- Recrediting Centre Id, the source of the request
- PSD Id, the Id of the PSD to which the Credit Certificate is to apply
- the source of the signature using the Recrediting Key covering the above data.

The KDC must check:

- the Recredit Authorisation Identifier
- that the PSD is associated with that requesting Recrediting Centre
- that it wishes to provide a Credit Certificate for the identified PSD and RF
- that the signature for the message is valid.

Recredit Authorisation Response Message

The KDC sends a Recredit Authorisation Response to the RF. The Recredit Authorisation Response Message contains a Credit Certificate and possibly also PSD control and key update instructions to be passed on to the PSD.

- Key Update of Blocks (a possibly empty sequence)
- PSD Control Block (optional)
- Credit Certificate.

The RF stores the information from this message. When any of the optional fields is present they must be included in the next Recredit Response Message sent to the PSD.

Referring to Figure 10, this is a flow chart illustrating essential data transmissions of the recredit protocol and recredit authorisation protocol. The CAF or KDC 14 has a cryptographic key pair comprising a secret key 50 and a public key 51 which is available to the user. A credit certificate 52 is transmitted from KDC 14 to RF and comprises information as to the total value that may be recredited 54, the public key 56 that the RF should use when transmitting information to the user, and a signature 58 which is based on a hash of the information in the credit certificate, hashed with the secret key 50 of the KDC.

The RF processes the credit certificate simply for verification and for storing the information in readiness for a user request. When a user makes a request in accordance with the protocol shown in Figure 3, the RF transmits a block of

data 60 into the user PSD 8 which includes information 62 as to the new credit limit for the PSD, and a digital signature 64 based on the information in the data block as hashed by the secret key of the RF which secret key 60 is generated from the public key 56. This thus provides a highly secure and reliable means of credit authorisation for the user and which maintains control by the postal supplier, the RF only being involved to the extent necessary to transmit the information, as and when required, to the user. The RF has discretion up to the limit specified in the CC for transmitting funds to the PSO.

The KDC 14 may frequently require updated keys to be sent to the various elements of the system. Figure 11 shows this updating mechanism. Four sets of data are provided A. B, C, D between limits P1, P2, P3, P4, P5 and P6. Each data unit comprises 500 numbers. The numbers in sector C correspond to the key version in sector A denoted as 1-500. The numbers in sector D correspond to those in sector B, denoted as 501-1000.

During the first period A, which might typically span 6 months, a set of encryption keys will be allocated to the first half of the 1000 keys version numbers. An encryption key along with its key version number will be transferred the first time each PSD is recredited during this period. In addition, a key expiry date will be down-loaded to the PSD corresponding to the end of the next key period. Up to this time an equivalent key will be referenced by the same key version number during indicia verification.

The key on the PSD must be changed during period B either the first time recrediting takes place or after a key change request is made. The encryption key allocated this time will be referenced by one of the second half of 1000 key

version numbers. This process will be repeated each subsequent period for each PSD. At the beginning of each new period new encryption keys will be allocated alternately to each half of the key version number range.

If each period lasts 6 months the above process will result in each PSD having to change its key at least once a year. If keys are not changed before their expiry dates then mail may be rejected following indicia verification. The real-time clock on the host device will be used to assist the customer to change keys at the appropriate intervals. During recrediting it will be checked using the system real-time clock and the printing of indicia will be disabled if a key passes its expiry date.

The PSD holds the date at which the key must be changed.

The present invention therefore provides a postal system with a recrediting system which at least in the preferred embodiment has the following features:

1. A protocol for recrediting PSDs from a recrediting centre, using Credit Certificates from a KDC.

2. The use of Credit Certificates to allow RFs to operate in a store-and-forward mode.

3. The use of Credit Certificates cryptographically signed by the KDC, to control recrediting activities and to eliminate risk of unauthorised credit creation.

4. The use of credit certificates to limit possible credit throughput in an individual PSD.

5. The use of key version identifiers prevent recrediting of PSDs, in an inconsistent or non-current cryptographic state.

6. Cryptographically binding key identifiers and key update blocks credit certificates to ensure that a PSD is updated to a consistent and current cryptographic state.

7. The use of a control block to allow the PSD to perform a limited class of operations at the instigation of the KDC.

CLAIMS

1. A postal franking system comprising:

postal franking means (PFM) including a postal security device (PSD) which maintains in a secure manner funds credit data;

a recrediting facility (RF) arranged to receive funds credit authorisation and to issue a funds credit response to the PSD in an encrypted and/or signed or authenticated form;

a credit authorisation facility (CAF) for issuing said funds credit authorisation for the PSD to be held by the RF; and

the PFM being operable to issue a funds credit request to the RF. and to receive the credit response.

2. A postal franking system according to claim 1, wherein the RF is responsive to a request from the PFM to check on the funds credit available to the PSD and to provide to the PFM the requested funds credit.

3. A system according to claim 1 or 2, wherein the CAF is arranged to provide to the RF a credit certificate including information on a limit on funds and including a digital signature or MAC based on a hash of information in the certificate using a secret key of the CAF, wherein the RF is arranged to store said credit certificate but not to verify the digital signature or MAC.

4. A system according to claim 3 wherein the PSD contains a public version of the key of the CAF and the RF is arranged to provide to the PFM in said funds credit response the first digital signature from the CAF so that the PSD can verify the first digital signature.

5. A system according to any preceding claim wherein the RF in said funds credit response is arranged to provide a digital signature based on a hash of the information therein using a secret key of the RF, and wherein the PSD is arranged to verify the second digital signature with a public key version of the key of the RF.

6. A postal franking system according to any preceding claim, wherein a user PSD is recredited in accordance with a protocol wherein the PSD communicates with the PFM to permit the PFM to generate an unsigned message for recrediting to the RF, and wherein in response to said recredit request message, the RF issues to the user PSD a recredit response message including said value of postal credits in signed form.

7. A postal system according to claim 6 wherein the user PSD is arranged to provide to said PFM, one or more items of information including the identity of the PSD, key versions held by the PSD, the CAF master key version held by the PSD, total value credited held by the PSD, total value spent held by PSD, in order that the PFM may construct therefrom a recredit request message, and wherein PFM is arranged to instruct a funds credit request which includes one or more items of the above information and in addition a requested value to be added to the total value credited.

8. A postal franking system according to claim 6 or 7 wherein the funds credit response message includes a recredit response block, and optionally a key update block and/or a PSD control block.

9. A postal franking system according to claim 8 wherein the key update

block if present comprises new values for cryptographic keys held by the PSD and includes a new key version identifier for the updated keys and/or encrypted keys to be replacements, and a signature using a CAF private key based on such data.

10. A postal franking system according to claim 8 or 9 wherein the PSD control block includes the PSD identity, one or more instructions indicating actions the PSD should perform, and a signature using a CAF private key covering such data.

11. A postal franking system according to claims 8, 9 or 10, wherein a recredit response block includes the PSD identifier, indications of the key versions after all key update operations had been performed, a new total value credited, and a signature using recrediting private key based on such data.

12. A postal franking system according to any preceding claim, wherein the PSD contains a first register containing the total value credited, that has ever been credited to the PSD, and a second register containing the total value spent, the total value of indicia that have ever been produced by the PSD.

13. A postal franking system according to any preceding claim, wherein the PSD contains a public version of a master key of the CAF, and a key version identifier to identify the version of the master key.

14. A method of issuing postal funds credit to users in a postal franking system, the postal franking system comprising:

postal franking means (PFM) including a postal security device

(PSD) which maintains in a secure manner funds credit data;

a credit authorisation facility (CAF);

a recrediting facility (RF) for issuing a funds credit to the PSD;

the method comprising the following steps:

(d) the CAF issuing to the RF a funds credit authorisation for the PSD;

(e) the PFM making to the RF a request for funds credit; and

(f) the RF issuing to the PSD, a funds credit response by means of a message encrypted and/or signed or authenticated form.

15. A method according to claim 14 wherein in step a), the CAF issues to the RF a limit on funds which may be credited to the PSD, and in step c), the RF checks on the funds available to the PSD prior to issuing said funds credit response.

16. A method according to claim 15, where the CAF provides said limit on funds to the RF in the form of a credit certificate (CC) exclusive to a PSD and including a digital signature based on a hash of information in the certificate using a secret key of the CAF, the RF storing the CC.

17. A method according to claim 16 wherein in step (c), the RF provides to the PFM said message including said digital signature, and the PSD containing the public version of the CAF key whereby the PSD verifies said digital signature.

18. A method according to any of claims 14 to 17 wherein in step (c) the RF

sends a digital signature based on a hash of the information therein using a secret key of the RF and wherein the PSD verifies this second mentioned digital signature with a public key version of the RF.

19. A method according to claim 17 wherein the RF public key used by the PSD is included in said message.

20. A method according to any of claims 14 to 19 wherein the CAF is arranged to distribute updated keys to the PSD and/or RF, encrypted with a transport key, and the PSD and/or includes a public version of the transport key for the encrypted updated keys.

21. A method according to claim 20 as dependent on claim 16 wherein the updated key is included in the credit certificate.

22. A method according to claim 19 or 20, wherein the PFM requests at regular intervals an updated key from the CAF.

23. A method according to any of claims 16 to 22, wherein the CAF is arranged to make available an updated key for the PSD by the following method:

(i) in a first time period a first set of key versions is allocated, and a key version is selected from the first set; each key version identifying a collection of keys, deriving keys held by PSDs from these keys which are determined from said key version and from a PSD identifier which is used to derive PSD – specific keys from the master key, and during this first time period if the PSD is recredited the updated key is transferred

with the funds audit response;

(iii) during a second time period, overlapping in part with the first time period, a second set of key versions is provided. and an updated key version is selected from the second set; and

wherein during the second time period the PSD key is changed either upon recrediting or following a key change request from the PFM.

24. A method according to claim 23 wherein in a third time period overlapping in part with the second time period an updated key is selected from the first set of keys versions. and wherein in a fourth time period overlapping in part with the third time period a revised key is selected from said second set of key versions.

25. A method according to claim 16, wherein in step (a), the CAF provides to the RF one or more of the following items of information: a PSD control block, and a PSD key update.

26. A method according to claim 16, wherein a credit certificate issued to a RF includes the identity of the user PSD to whom the credit certificate is applicable, cryptographic key versions identifiers applicable to the user PSD, and the total value which the RF may assign to the user PSD.

27. A method according to any of claims 14 to 26 wherein in step (b), a user PSD provides one or more of the following items of information to the user PFM: the PSD identity, key versions held by the PSD, and total value credited by the PSD; and from such information, the PFM constructs a recredit request message which is sent to the RF, including in addition a requested value to be

added to the PSDs total value credited.

28. A method according to any of claims 14 to 27 wherein in step (c), a fund credit response message includes one or more of a key update block. a PSD control block, and a recredit response block.

29. A method according to claim 28 wherein the key update block includes one or more of the following items of information:

A key update indicator, the user PSD. new key versions for updated keys and encrypted keys for replacement keys, and a signature using a CAF master key performing a hash on the aforesaid data. and wherein the user PSD checks the above items of information.

30. A method according to claim 28 or 29 wherein the PSD control block includes one or more of the following items of information:

a PSD control block indicator, the identity of the intended PSD, an instruction indicating an action the PSD should perform, and a signature based on hash of the aforesaid data using a postal service master key, and wherein on receiving a PSD control block, the PSD checks the information and verifies the signature is correct, and performs the aforesaid instruction if applicable.

31. A method according to claims 28, 29 or 30 wherein the recredit response block contains one or more of the following items of information: A recredit response indicator, the identity of the user PSD, the key versions after all key update operations have been performed, a new total value credited, a signature using a recrediting key based on a hash of the aforesaid data, and a credit

certificate for the recrediting key, and wherein in response to the response block, the PSD accepts the new total value credited if and only if the information in the block is verified, if the key versions match those held in the PSD, if the total value credited is greater than that held by the PSD, if the limit of total value credited is not less than the new total value credited, if the recrediting public key can verify the signature in the recredit response block. and if the supply master public key held by PSD can verify the signature in the credit certificate.

32. A method according to any of claims 14 to 31, wherein the PSD contains a first register containing the total value credited, that has ever been credited to the PSD, and a second register containing the total value spent, the total value of indicia that have ever been produced by the PSD.

33. A method according to any of claims 14 to 32, wherein the PSD contains a public version of a master key of the CAF, and a key version identifier to identify the version of the master key.

34. A method of issuing postal credit values to users in a postal franking system, the postal franking system including:

postal franking means (PFM) including a postal security device (PSD) for maintaining in a secure manner funds credit data;

a recrediting facility(RF) for issuing a funds credit to the PSD;

wherein the method comprises:-

(a) the PFM issuing to the RF an unsigned request message for the reallocation of funds to the user PSD;

(b) in response thereto the RF providing a response message including a new reallocation of funds and the message including a signature based on encrypting a hash of the information in the message with a key of the RF and including credit information having a second signature formed by encrypting a hash of the credit information using a second key;

(c) the PSD means verifying the response message and verifying the message using the first key of the RF and the second key; and

wherein the user PSD stores in a secure manner the revised funds allocation information.

35. A method of updating keys for use in a secure postal franking system, as follows:

(i) in a first time period a first set of key versions is allocated, and a key version is selected from the first set; each key version identifying a collection of keys;

(ii) deriving keys held by a security device from these keys which are determined from the identifying key version and from a security device identifier, and during this first time period if the security device is operated, the updated key is transferred thereto;

(iv) during a second time period, overlapping in part with the first time period, a second set of key versions is provided, and an updated key version is selected from the second set; and

wherein during the second time period the security device key is changed either upon operation or following a key change request.

36. A postal security device adapted for use in a system or method as claimed in any of the preceding claims.

37. A postal security device as claimed in claim 36, wherein the device is a smart card.

AMENDED CLAIMS

CLAIMS [received by the International Bureau on 7 August 2000 (07.08.00); original claims 1-37 replaced by amended claims 1-38 (9 pages)]

1. A postal franking system comprising:

postal franking means (PFM) including a postal security device (PSD) which maintains in a secure manner funds credit data;

a re-crediting facility (RF) arranged to receive funds credit authorisation and to issue a funds credit response to the PSD in an encrypted and/or signed or authenticated form, the PFM being operable to issue a funds credit request to the RF, and to receive the credit response; and

a credit authorisation facility (CAF) for issuing said funds credit authorisation for the PSD to be held by the RF in the form of a credit certificate, wherein the funds credit response issued to the PSD includes at least a portion of the credit certificate, which portion is verifiable by the PSD.

2. A postal franking system according to claim 1, wherein the RF is responsive to a request from the PFM to check on the funds credit available to the PSD and to provide to the PFM the requested funds credit.

3. A system according to claim 1 or 2, wherein the credit certificate includes information on a limit on funds and a digital signature or MAC based on a hash of information in the certificate using a secret key of the CAF, wherein the RF is arranged to store said credit certificate but not to verify the digital signature or MAC.

4. A system according to claim 3 wherein the PSD contains a public version of the key of the CAF and the RF is arranged to provide to the PFM in said funds credit response the first digital signature from the CAF so that the PSD can verify the first digital signature.

5. A system according to any preceding claim wherein the RF in said funds credit response is arranged to provide a digital signature based on a hash of the information therein using a secret key of the RF, and wherein the PSD is arranged to verify the second digital signature with a public key version of the key of the RF.

6. A postal franking system according to any preceding claim, wherein a user PSD is recredited in accordance with a protocol wherein the PSD communicates with the PFM to permit the PFM to generate an unsigned message for recrediting to the RF, and wherein in response to said recredit request message, the RF issues to the user PSD a recredit response message including said value of postal credits in signed form.

7. A postal system according to claim 6 wherein the user PSD is arranged to provide to said PFM, one or more items of information including the identity of the PSD, key versions held by the PSD, the CAF master key version held by the PSD, total value credited held by the PSD, total value spent held by PSD, in order that the PFM may construct therefrom a recredit request message, and wherein PFM is arranged to instruct a funds credit request which includes one or more items of the above information and in addition a requested value to be added to the total value credited.

8. A postal franking system according to claim 6 or 7 wherein the funds credit response message includes a recredit response block, and optionally a key update block and/or a PSD control block.

9. A postal franking system according to claim 8 wherein the key update block if present comprises new values for cryptographic keys held by the PSD and includes a new key version identifier for the updated keys and/or encrypted keys to be replacements, and a signature using a CAF private key based on such data.

10. A postal franking system according to claim 8 or 9 wherein the PSD control block includes the PSD identity, one or more instructions indicating actions the PSD should perform, and a signature using a CAF private key covering such data.

11. A postal franking system according to claims 8, 9 or 10, wherein a recredit response block includes the PSD identifier, indications of the key versions after all key update operations had been performed, a new total value credited, and a signature using recrediting private key based on such data.

12. A postal franking system according to any preceding claim, wherein the PSD contains a first register containing the total value credited, that has ever been credited to the PSD, and a second register containing the total value spent, the total value of indicia that have ever been produced by the PSD.

13. A postal franking system according to any preceding claim, wherein the PSD contains a public version of a master key of the CAF, and a key version identifier to identify the version of the master key.

14. A method of issuing postal funds credit to users in a postal franking system, the postal franking system comprising:

postal franking means (PFM) including a postal security device (PSD) which maintains in a secure manner funds credit data;

a credit authorisation facility (CAF);

a recrediting facility (RF) for issuing a funds credit to the PSD;

the method comprising the following steps:

(a) the CAF issuing to the RF a funds credit authorisation for the PSD, in the form of a credit certificate;

(b) the PFM making to the RF a request for funds credit; and

(c) the RF issuing to the PSD, a funds credit response by

means of a message encrypted and/or signed or authenticated form, wherein the funds credit response includes a portion of the credit certificate that is verifiable by the PSD.

15. A method according to claim 14 wherein in step a), the credit certificate includes a limit on funds which may be credited to the PSD, and in step c), the RF checks on the funds available to the PSD prior to issuing said funds credit response.

16. A method according to claim 15, wherein the credit certificate (CC), which is exclusive to a PSD, includes a digital signature based on a hash of information in the certificate using a secret key of the CAF, the RF storing the CC.

17. A method according to claim 16 wherein in step (c), the RF provides to the PFM said message including said digital signature, and the PSD containing the public version of the CAF key whereby the PSD verifies said digital signature.

18. A method according to any of claims 14 to 17 wherein in step (c) the RF sends a digital signature based on a hash of the information therein using a secret key of the RF and wherein the PSD verifies this second mentioned digital signature with a public key version of the RF.

19. A method according to claim 17 wherein the RF public key used by the PSD is included in said message.

20. A method according to any of claims 14 to 19 wherein the CAF is arranged to distribute updated keys to the PSD and/or RF, encrypted with a transport key, and the PSD and/or includes a public version of the transport key

for the encrypted updated keys.

21. A method according to claim 20 as dependent on claim 16 wherein the updated key is included in the credit certificate.

22. A method according to claim 19 or 20, wherein the PFM requests at regular intervals an updated key from the CAF.

23. A method according to any of claims 16 to 22, wherein the CAF is arranged to make available an updated key for the PSD by the following method:

(i) in a first time period a first set of key versions is allocated, and a key version is selected from the first set; each key version identifying a collection of keys, deriving keys held by PSDs from these keys which are determined from said key version and from a PSD identifier which is used to derive PSD – specific keys from the master key, and during this first time period if the PSD is recredited the updated key is transferred with the funds audit response;

(ii) during a second time period, overlapping in part with the first time period, a second set of key versions is provided, and an updated key version is selected from the second set; and

wherein during the second time period the PSD key is changed either upon recrediting or following a key change request from the PFM.

24. A method according to claim 23 wherein in a third time period overlapping in part with the second time period an updated key is selected from the first set of keys versions, and wherein in a fourth time period overlapping in part with the third time period a revised key is selected from said second set of key versions.

25. A method according to claim 16, wherein in step (a), the CAF provides to the RF one or more of the following items of information: a PSD control block, and a PSD key update.

26. A method according to claim 16, wherein a credit certificate issued to a RF includes the identity of the user PSD to whom the credit certificate is applicable, cryptographic key versions identifiers applicable to the user PSD, and the total value which the RF may assign to the user PSD.

27. A method according to any of claims 14 to 26 wherein in step (b), a user PSD provides one or more of the following items of information to the user PFM: the PSD identity, key versions held by the PSD, and total value credited by the PSD; and from such information, the PFM constructs a recredit request message which is sent to the RF, including in addition a requested value to be added to the PSDs total value credited.

28. A method according to any of claims 14 to 27 wherein in step (c), a fund credit response message includes one or more of a key update block, a PSD control block, and a recredit response block.

29. A method according to claim 28 wherein the key update block includes one or more of the following items of information:

A key update indicator, the user PSD, new key versions for updated keys and encrypted keys for replacement keys, and a signature using a CAF master key performing a hash on the aforesaid data, and wherein the user PSD checks the above items of information.

30. A method according to claim 28 or 29 wherein the PSD control block includes one or more of the following items of information:

a PSD control block indicator, the identity of the intended PSD, an

instruction indicating an action the PSD should perform, and a signature based on hash of the aforesaid data using a postal service master key, and wherein on receiving a PSD control block, the PSD checks the information and verifies the signature is correct, and performs the aforesaid instruction if applicable.

31. A method according to claims 28, 29 or 30 wherein the recredit response block contains one or more of the following items of information:

a recredit response indicator, the identity of the user PSD, the key versions after all key update operations have been performed, a new total value credited, a signature using a recrediting key based on a hash of the aforesaid data, and a credit certificate for the recrediting key, and wherein in response to the response block, the PSD accepts the new total value credited if and only if the information in the block is verified, if the key versions match those held in the PSD, if the total value credited is greater than that held by the PSD, if the limit of total value credited is not less than the new total value credited, if the recrediting public key can verify the signature in the recredit response block, and if the supply master public key held by PSD can verify the signature in the credit certificate.

32. A method according to any of claims 14 to 31, wherein the PSD contains a first register containing the total value credited, that has ever been credited to the PSD, and a second register containing the total value spent, the total value of indicia that have ever been produced by the PSD.

33. A method according to any of claims 14 to 32, wherein the PSD contains a public version of a master key of the CAF, and a key version identifier to identify the version of the master key.

34. A method of issuing postal credit values to users in a postal franking system, the postal franking system including:

postal franking means (PFM) including a postal security device (PSD) for maintaining in a secure manner funds credit data;

a recrediting facility(RF) for issuing a funds credit to the PSD;

wherein the method comprises:-

(a) the PFM issuing to the RF an unsigned request message for the reallocation of funds to the user PSD;

(b) in response thereto the RF providing a response message including a new reallocation of funds and the message including a signature based on encrypting a hash of the information in the message with a key of the RF and including credit information having a second signature formed by encrypting a hash of the credit information using a second key;

(c) the PSD means verifying the response message and verifying the message using the first key of the RF and the second key; and

wherein the user PSD stores in a secure manner the revised funds allocation information.

35. A postal franking system comprising postal franking means (PFM) including a postal security device (PSD) for maintaining in a secure manner funds credit data, and a recrediting facility (RF) for issuing a funds credit to the PSD, wherein the PFM is operable to issue to the RF an unsigned request message for the reallocation of funds to the user PSD and in response thereto the RF is operable to provide a response message including a new reallocation of funds, the response message including a signature based on encrypting a hash of the information in the message with a key of the RF and including credit information having a second signature formed by encrypting a hash of the credit information using a second key; the PSD being operable to verify the response message using the first key of the RF and the second key and to store

in a secure manner the revised funds allocation information.

36. A method of updating keys for use in a secure postal franking system, as follows:

(i) in a first time period a first set of key versions is allocated, and a key version is selected from the first set; each key version identifying a collection of keys;

(ii) deriving keys held by a security device from these keys which are determined from the identifying key version and from a security device identifier, and during this first time period if the security device is operated, the updated key is transferred thereto;

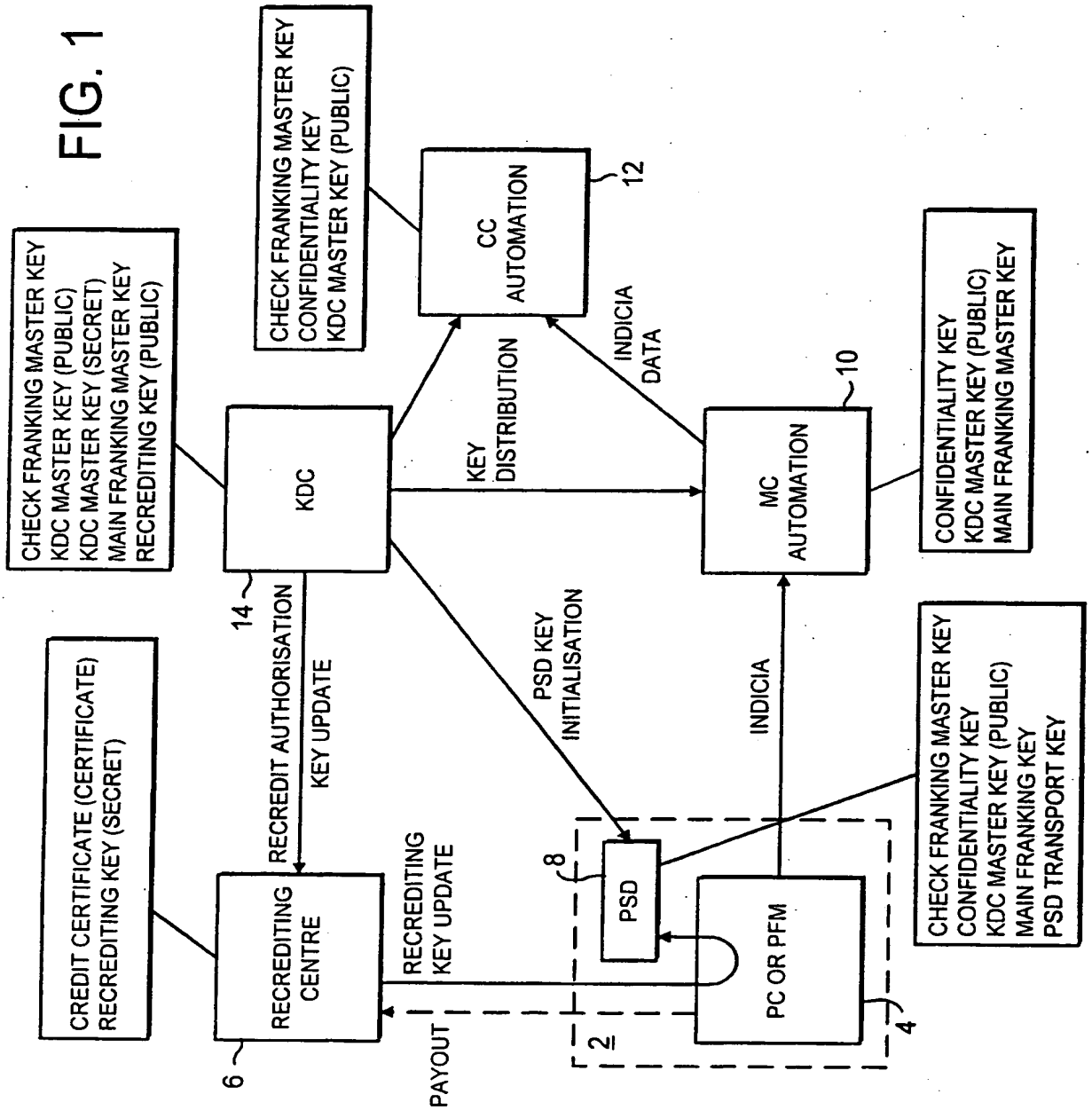
(iii) during a second time period, overlapping in part with the first time period, a second set of key versions is provided, and an updated key version is selected from the second set; and

wherein during the second time period the security device key is changed either upon operation or following a key change request.

37. A postal security device adapted for use in a system or method as claimed in any of the preceding claims.

38. A postal security device as claimed in claim 36, wherein the device is a smart card.

FIG. 1


CHECK FRANKING MASTER KEY
KDC MASTER KEY (PUBLIC)
KDC MASTER KEY (SECRET)
MAIN FRANKING MASTER KEY
RECREDITING KEY (PUBLIC)
CHECK FRANKING MASTER KEY
CONFIDENTIALITY KEY
KDC MASTER KEY (PUBLIC)
CC AUTOMATION
12
KDC
KEY DISTRIBUTION
INDICIA DATA
MC AUTOMATION
10
CONFIDENTIALITY KEY
KDC MASTER KEY (PUBLIC)
MAIN FRANKING MASTER KEY
14
RECREDIT AUTHORISATION
KEY UPDATE
PSD KEY INITIALISATION
INDICIA
CREDIT CERTIFICATE (CERTIFICATE)
RECREDITING KEY (SECRET)
RECREDITING CENTRE
RECREDITING KEY UPDATE
8
PSD
PC OR PFM
CHECK FRANKING MASTER KEY
CONFIDENTIALITY KEY
KDC MASTER KEY (PUBLIC)
MAIN FRANKING KEY
PSD TRANSPORT KEY
6
PAYOUT
2
4

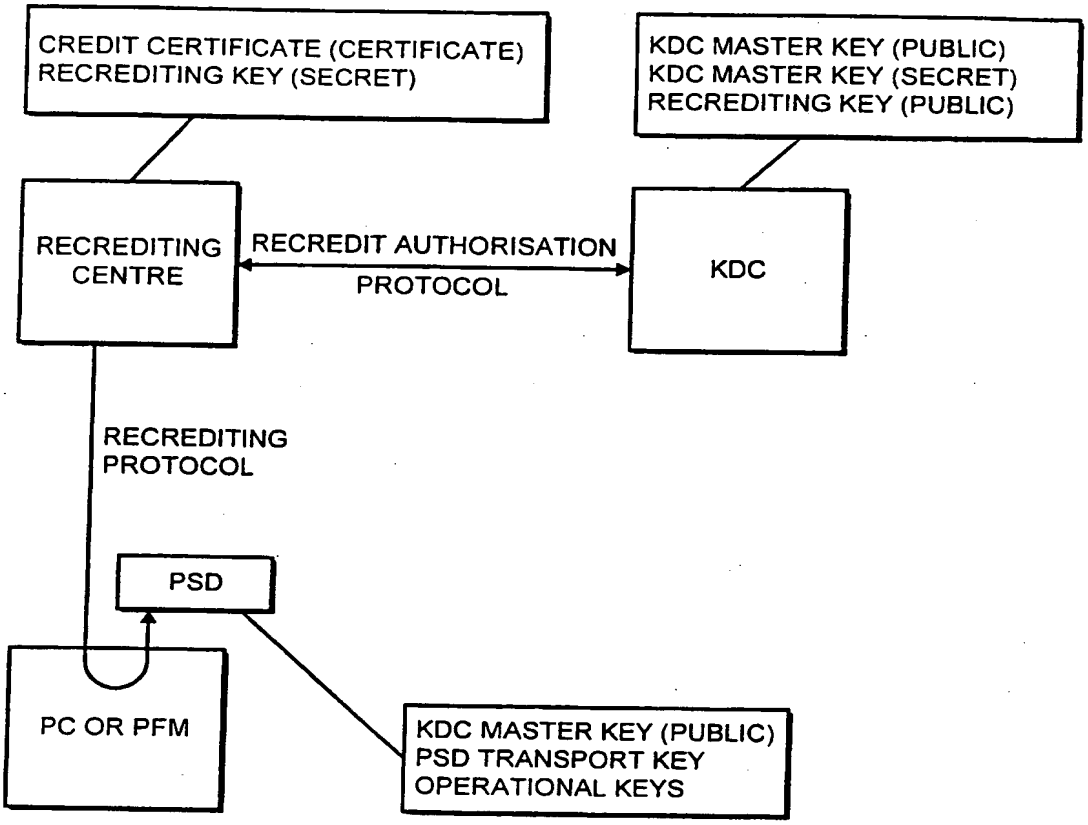
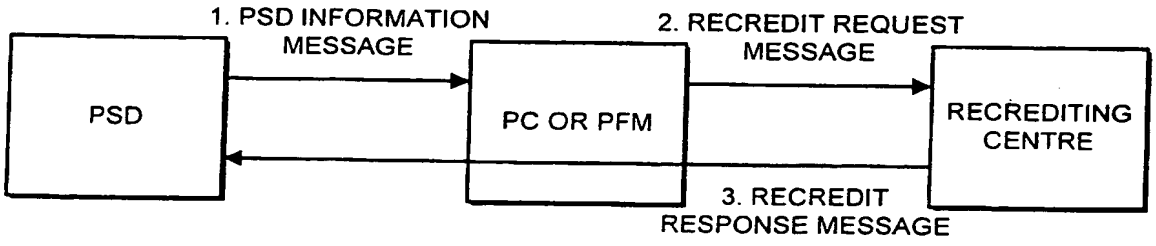


FIG. 2

FIG. 3

THE RECREDITING PROTOCOL



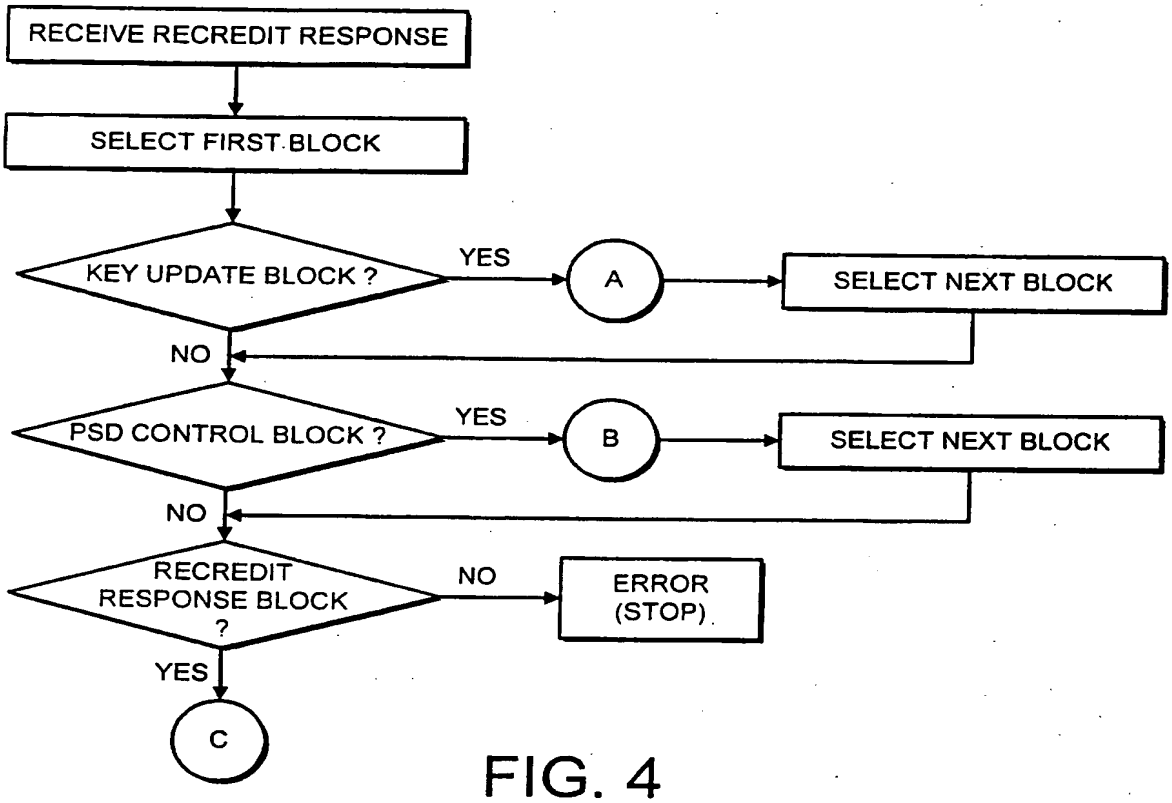


FIG. 4

PROCESSING A RECREDIT RESPONSE MESSAGE IN A PSD

FIG. 5

PROCESSING A RECREDIT RESPONSE -THE KEY UPDATE BLOCK IN A PSD

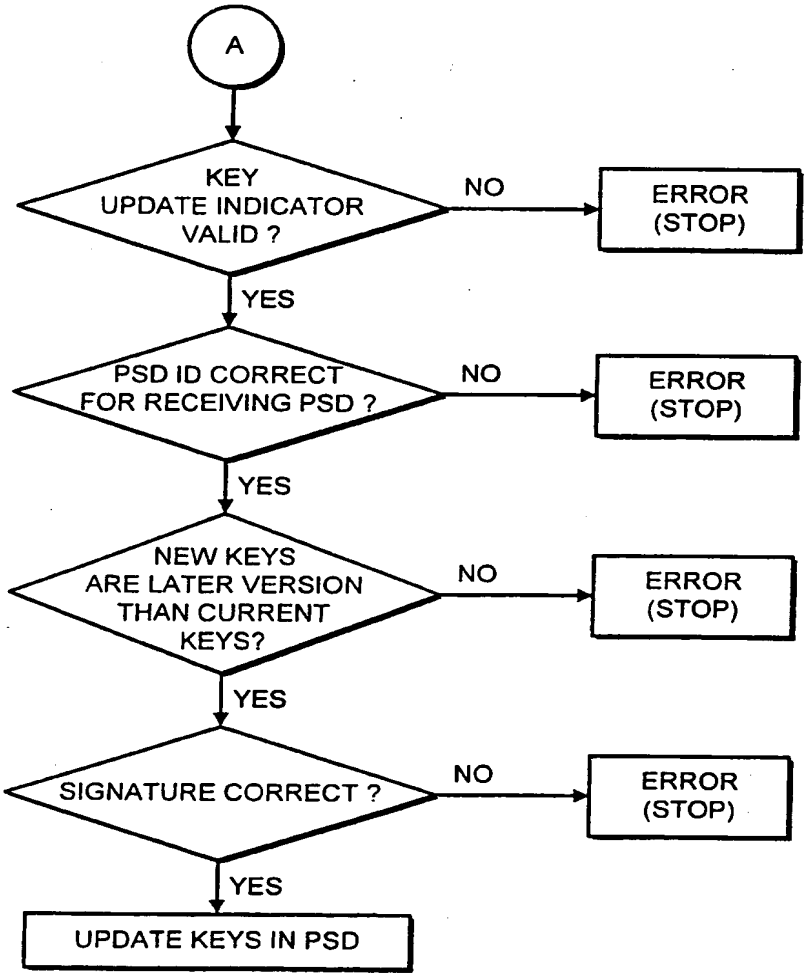


FIG. 6

PROCESSING A RECREDIT RESPONSE -THE PSD CONTROL BLOCK IN A PSD

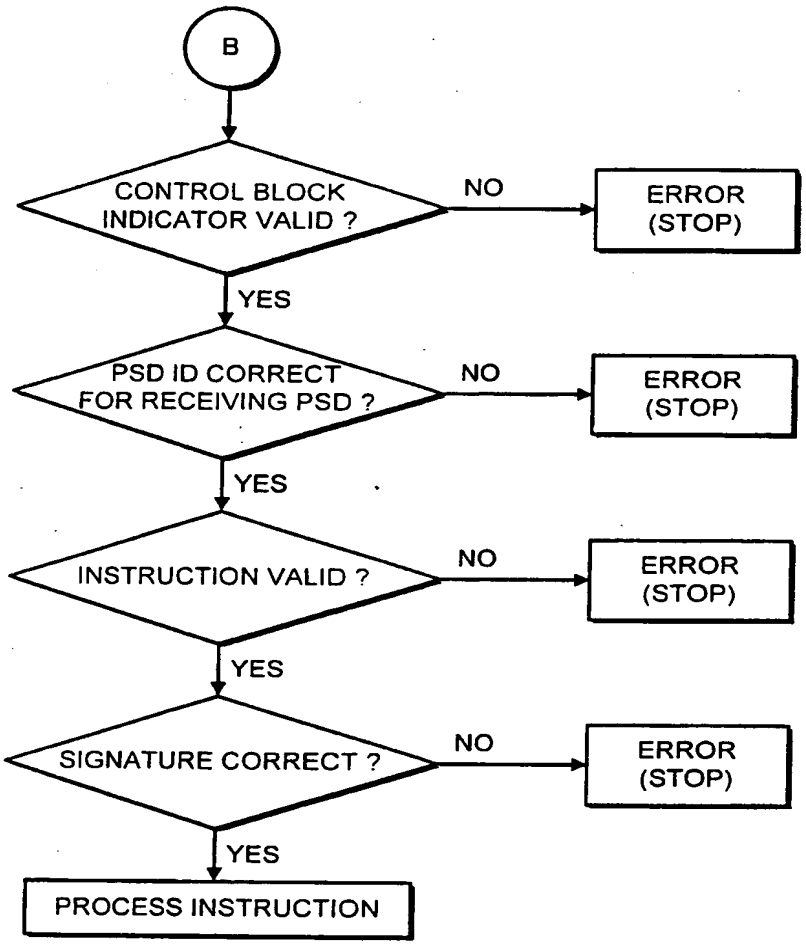


FIG. 7

PROCESSING A RECREDIT RESPONSE -THE RECREDIT RESPONSE BLOCK IN A PSD

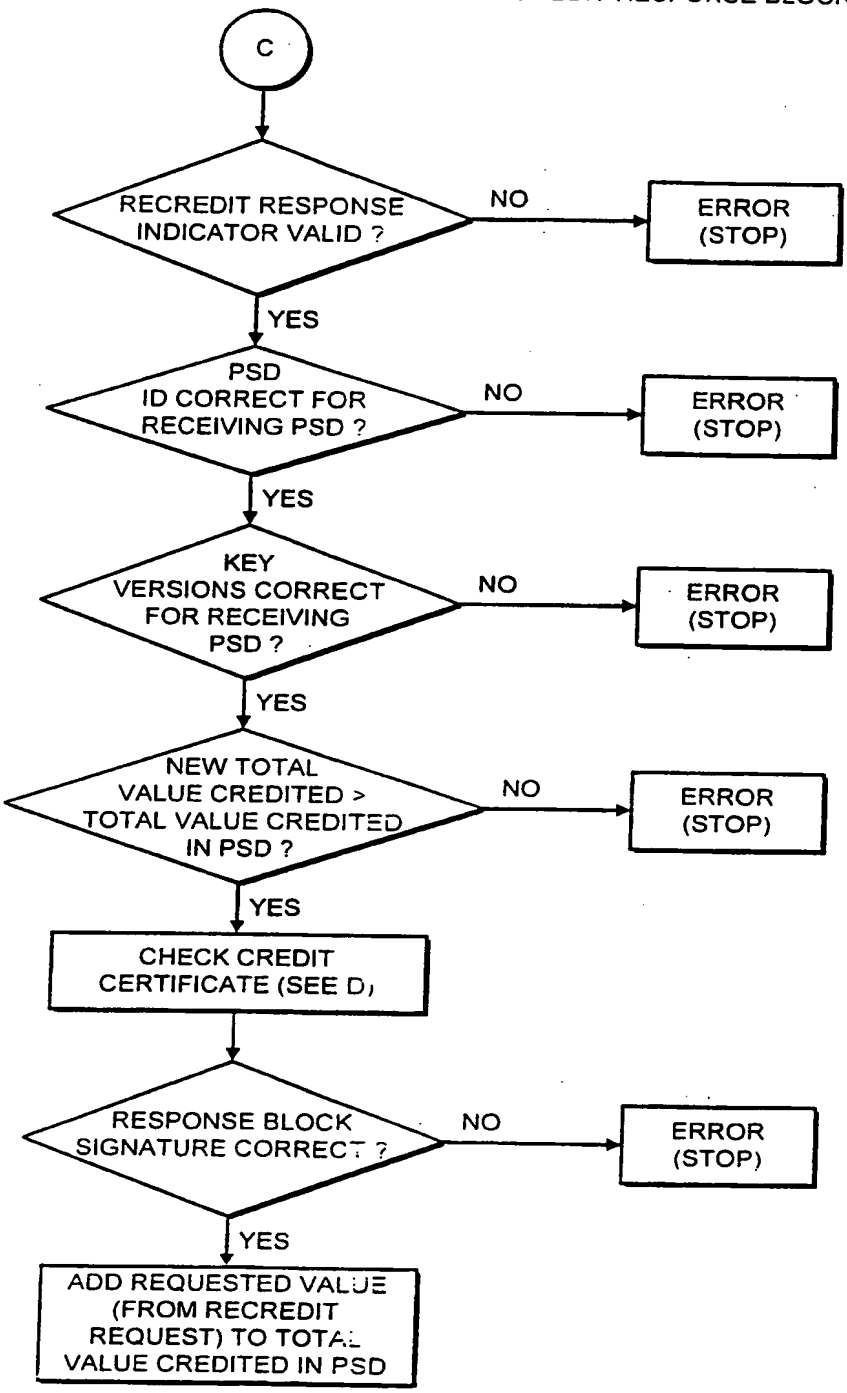


FIG. 8

PROCESSING A RECREDIT RESPONSE -THE CREDIT CERTIFICATE

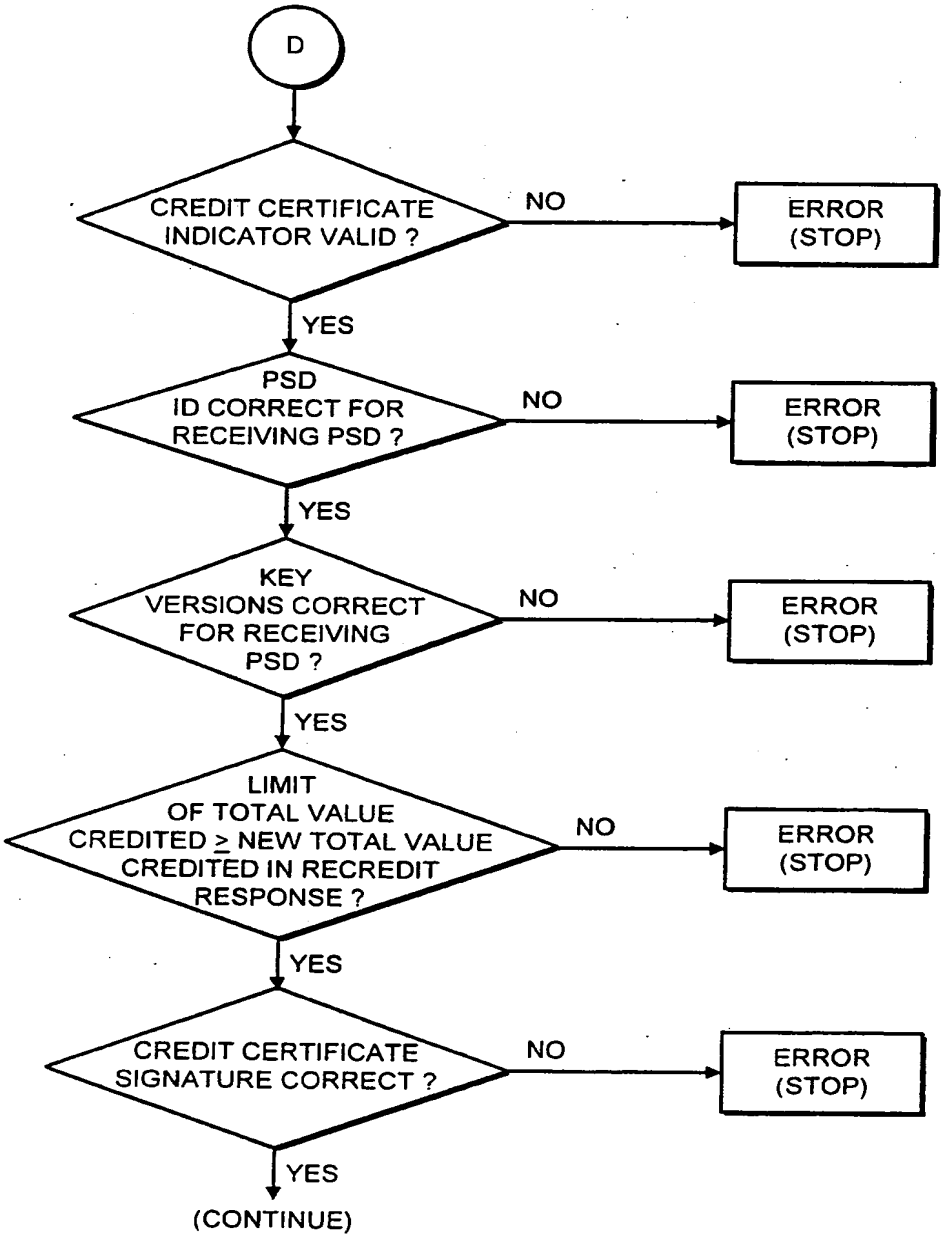
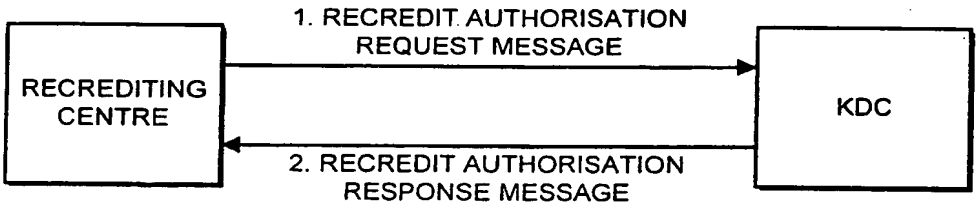


FIG. 9

THE RECREDIT AUTHORISATION PROTOCOL



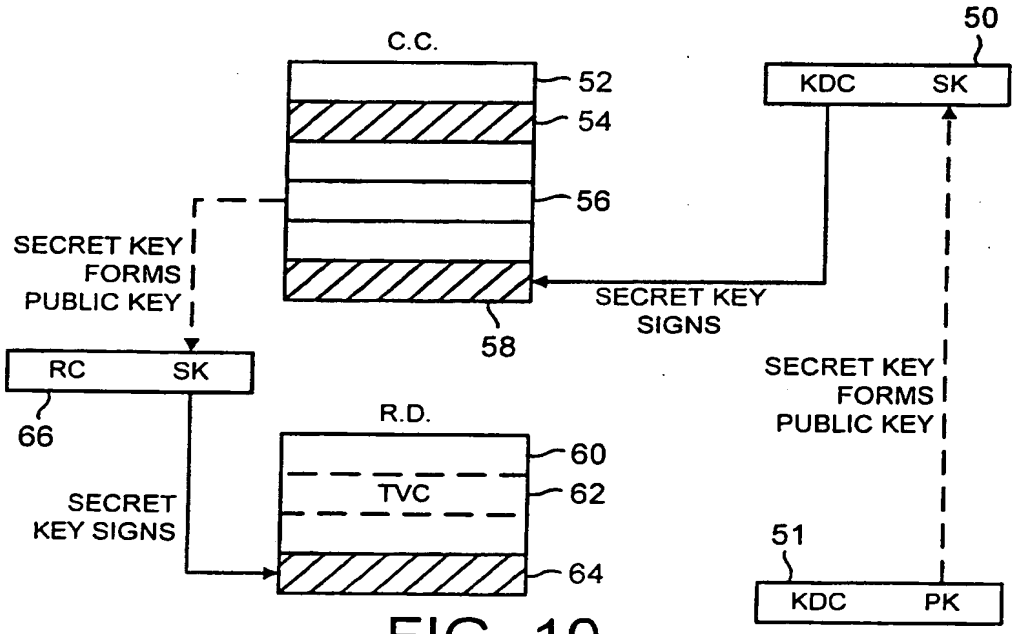


FIG. 10

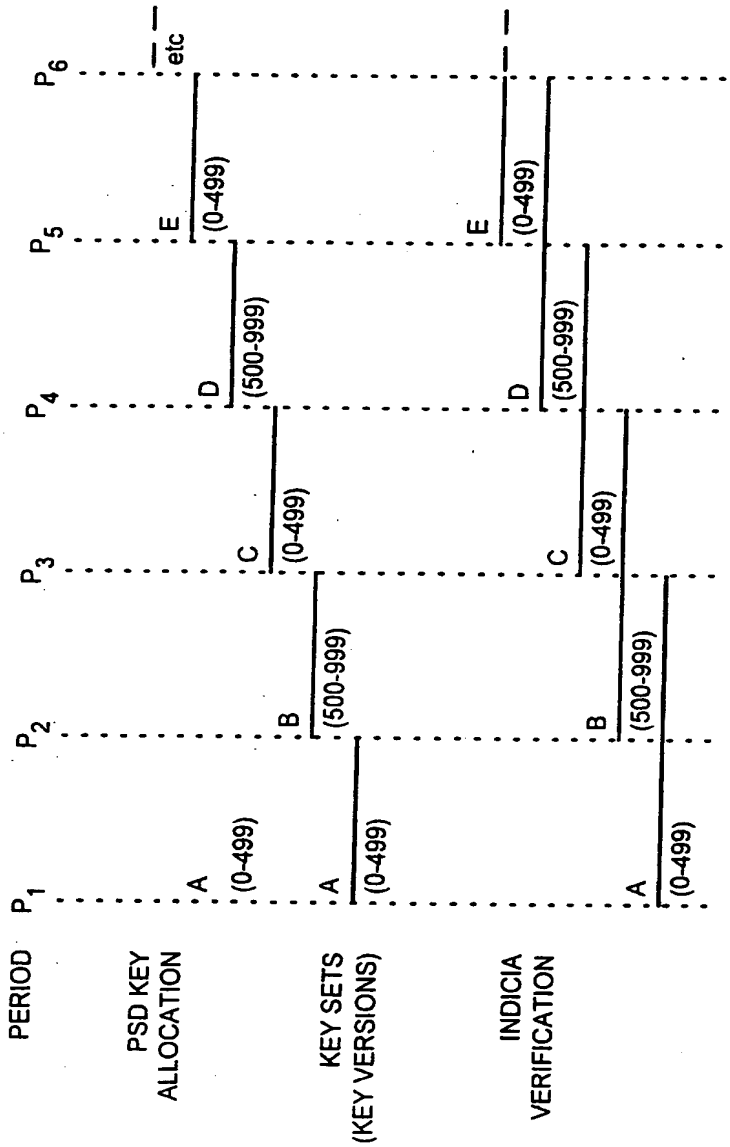

PERIOD
PSD KEY ALLOCATION
KEY SETS (KEY VERSIONS)
INDICIA VERIFICATION
P1
P2
P3
P4
P5
P6
A
B
C
D
E
(0-499)
(500-999)
(0-499)
(500-999)
(0-499)
(500-999)
(0-499)
(500-999)
(0-499)
etc

FIG. 11

INTERNATIONAL SEARCH REPORT

Inter[illegible]pplication No
PCT/GB 00/01041

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07B17/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	"Performance Criteria for Information-based Indicia and Security Architecture for Closed IBI Postage Metering systems (PCIBI-C)" 12 January 1999 (1999-01-12) , UNITED STATES POSTAL SERVICE XP002138350	1,2,14, 15,18
A	page II	3-13,16, 17,19-37
A	US 5 666 421 A (PASTOR JOSE ET AL) 9 September 1997 (1997-09-09) claim 1; figure 1	1-37
A	EP 0 854 444 A (PITNEY BOWES) 22 July 1998 (1998-07-22) claim 1; figure 1	1-37

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 May 2000	07/06/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Kirsten, K

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 854 446 A (PITNEY BOWES) 22 July 1998 (1998-07-22) claim 1; figure 3	1-37
A	EP 0 735 722 A (PITNEY BOWES) 2 October 1996 (1996-10-02) claim 1; figure 1	1-37
A	"Information Based Indicia Program (IBIP) PSD Specification" 13 June 1996 (1996-06-13) , UNITED STATES POSTAL SERVICE XP002137734 figure 2.1	1-37

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter[redacted] Application No
PCT/GB 00/01041

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5666421 A	09-09-1997	US 5390251 A	14-02-1995
		CA 2133497 A,C	09-04-1995
		EP 0649120 A	19-04-1995
EP 0854444 A	22-07-1998	US 5982896 A	09-11-1999
		CA 2222662 A	23-06-1998
		US 6058193 A	02-05-2000
EP 0854446 A	22-07-1998	US 5812990 A	22-09-1998
		CA 2224672 A	23-06-1998
EP 0735722 A	02-10-1996	US 5812666 A	22-09-1998
		BR 9601231 A	06-01-1998
		CA 2173008 A	01-10-1996
		CN 1147656 A	16-04-1997
		JP 9149021 A	06-06-1997